
Unicenter

NetSpy Network Performance Getting Started

Version 6.0

MAN06112621E



Computer Associates
The Software That Manages eBusiness



This documentation and related computer software program (hereinafter referred to as the "Documentation") is for the end user's informational purposes only and is subject to change or withdrawal by Computer Associates International, Inc. ("CA") at any time.

This documentation may not be copied, transferred, reproduced, disclosed or duplicated, in whole or in part, without the prior written consent of CA. This documentation is proprietary information of CA and protected by the copyright laws of the United States and international treaties.

Notwithstanding the foregoing, licensed users may print a reasonable number of copies of this documentation for their own internal use, provided that all CA copyright notices and legends are affixed to each reproduced copy. Only authorized employees, consultants, or agents of the user who are bound by the confidentiality provisions of the license for the software are permitted to have access to such copies.

This right to print copies is limited to the period during which the license for the product remains in full force and effect. Should the license terminate for any reason, it shall be the user's responsibility to return to CA the reproduced copies or to certify to CA that same have been destroyed.

To the extent permitted by applicable law, CA provides this documentation "as is" without warranty of any kind, including without limitation, any implied warranties of merchantability, fitness for a particular purpose or noninfringement. In no event will CA be liable to the end user or any third party for any loss or damage, direct or indirect, from the use of this documentation, including without limitation, lost profits, business interruption, goodwill, or lost data, even if CA is expressly advised of such loss or damage.

The use of any product referenced in this documentation and this documentation is governed by the end user's applicable license agreement.

The manufacturer of this documentation is Computer Associates International, Inc.

Provided with "Restricted Rights" as set forth in 48 C.F.R. Section 12.212, 48 C.F.R. Sections 52.227-19(c)(1) and (2) or DFARS Section 252.227-7013(c)(1)(ii) or applicable successor provisions.

© 2002 Computer Associates International, Inc. (CA)

All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Contents

Chapter 1: Introduction to NetSpy

What NetSpy Does	1-1
Evaluate Network Efficiency	1-2
Discover System Problems	1-2
Monitor TCP/IP Stack Workload	1-2
Monitor Service Level Agreements (SNA)	1-3
Analyze Network Capacity	1-3
Plan for Future Expansion	1-4
Who Benefits from NetSpy?	1-5
Network Control Center Staff	1-5
Systems Programmers	1-5
Help Desk Personnel	1-6
Management	1-7
Network Capacity Planners	1-7
Accounting Personnel	1-7
Related Documentation	1-8

Chapter 2: Release Summary

- New Primary Menu 2-2
- TCP/IP Performance Enhancements 2-3
 - Monitoring Critical IP Resources and Nodes 2-3
 - Other Enhancements for TCP/IP 2-5
- SNA Performance Enhancements 2-6
 - Integration with the NetMaster Alert Monitor 2-6
 - Improved Availability 2-6
 - NeuPerformance Advisor Interface 2-7
 - Other Enhancements for SNA 2-7
- Administration and Customization Enhancements 2-8

Chapter 3: Installing and Implementing the NetSpy Product

- Installation and Implementation Overview 3-2
- Step 1: Install and Set Up the Product 3-2
- Step 2: Customize the NetSpy SNA Agent 3-3
- Step 3: Implement the TCP/IP Interface 3-3
- Step 4: Build the Environment to Manage Your TCP/IP Resources 3-4
- Step 5: Implement Other Functions 3-4

Chapter 4: Quick Tour

- About The Quick Tour 4-1
- Examining Your IP Details 4-2
- Listing Telnet Connections 4-7
- Examining Stack Monitoring Setup 4-9
- Viewing the Monitoring Results 4-12

Index

Introduction to NetSpy

Unicenter NetSpy Network Performance, known as NetSpy, is a performance monitor for SNA and TCP/IP networks that measures end-to-end network performance and response time. NetSpy lets you optimize the use of your network by measuring the overall performance of both the host *and* the network, and by suggesting ways to improve performance. When your network is running efficiently, you save time and money.

What NetSpy Does

With NetSpy, you can accomplish the following tasks for your network environment:

- Evaluate network efficiency
- Discover system problems
- Monitor TCP/IP stack workload
- Monitor service level agreements (SNA)
- Analyze network capacity
- Plan for future network expansion

Evaluate Network Efficiency

As NetSpy monitors your network, it collects information about how the network is functioning. It gathers network and host response times and traffic and error statistics. Using this information, NetSpy can generate online (on-screen) and offline (printed) reports so that you may view the collected statistics or prepare presentations. These online and offline reports will help you analyze your network's performance to determine whether or not it is operating efficiently and to suggest what you can do to enhance performance.

Discover System Problems

High traffic and failing equipment can multiply system error rates, increasing end user response time. NetSpy assists help desk and network personnel to quickly determine whether the network or the mainframe causes system response time delays. If the network causes a delay, NetSpy can also pinpoint the specific cause of delay so that you can correct it. In some cases, NetSpy can even detect problems caused by poorly coded applications.

Monitor TCP/IP Stack Workload

Most companies are seeing increased TCP/IP traffic load on the OS/390 TCP/IP stack due to eBusiness initiatives. The ability to manage the OS/390 stack is important to status monitoring. If you can understand the workload associated with key functions, such as FTP and Telnet, then you are able to ensure a highly reliable service. NetSpy provides information about FTP, Telnet, and API client connection activity.

Monitor Service Level Agreements (SNA)

Suppose that you have established a service level objective of keeping user response rates below two seconds, based on a certain amount of network traffic. NetSpy will determine if your installation is meeting your response time targets, so that you can continue to provide satisfactory response time levels for your network users. This is especially important as the number of users and transaction rates on your system increases.

NetSpy also provides network session and gateway accounting for NCPs so that you can collect complete session statistics for your network.

Analyze Network Capacity

The more complex your network becomes, the greater the importance of network performance monitoring. By providing information on how hardware is being used, NetSpy can help you balance loads and suggest new ways to configure the network.

Using the statistics NetSpy provides, you can move terminals and other equipment from over-used circuits, thereby reducing traffic and response times.

Plan for Future Expansion

NetSpy not only collects data, but also goes a step beyond, letting you model network modifications on SNA boundary lines *before* you make them. With the modeling feature, you can alter network configuration statistics online and then observe the impact of these changes on network response and traffic times. NetSpy models the network scenarios you invent, providing you with the hypothetical response information you need to configure your network efficiently. This allows you to add, subtract, or redistribute control units, terminals, and other resources. With its recommendations feature, NetSpy can then recommend how to actually configure your network resources to improve response times.

With Modeling and Recommendations, future planning is more precise and cost effective. Being able to review the effects of network changes before actually implementing them allows you to eliminate ineffective plans.

Who Benefits from NetSpy?

Many people in your company can benefit from the performance indicators of NetSpy.

Network Control Center Staff

NetSpy is an important tool if you are responsible for the day-to-day management of your network.

NetSpy can alert you when network resources exceed specified thresholds that you have defined. Alert messages can be sent to a terminal, NetView, NetMaster, a system console, Unicenter via SNMP, a NetSpy log, or SMF.

NetSpy collects current information about network line use and error rates. It can then quickly identify failing or degrading network components. Because users do not always ask for help the day they first experience a problem, NetSpy lets you display historical as well as real-time data online.

Systems Programmers

NetSpy provides a wide range of current and historical statistics from VTAM, NCP, and TCP/IP including:

- Host and network response times
- Message sizes and numbers
- Transaction traces
- Virtual route statistics
- Traffic statistics for all nodes
- 37X5 processor and buffer use
- NCP slowdown times
- APPN statistics
- Token ring statistics

This historical data can be presented in detail or summarized displays, graphs, or reports. It is most useful in detecting problems and tuning the network over an extended period of time.

With NetSpy you can select transactions you want to trace by specifying response time thresholds for them. NetSpy monitors each transaction, measuring its host and network time. You can then compare the actual response time with your threshold.

NetSpy's modeling component allows you to use "what if" scenarios consisting of proposed changes to NCP, traffic, and hardware characteristics. You can then evaluate the impact of changes before making them. You can also use modeling to measure the improved performance you gain when you use NetSpy's recommendations.

NetSpy can also identify the most common elements of poorly designed applications that impact network resources and degrade response times (for example, when the modified data tag in the program code is not reset).

Help Desk Personnel

NetSpy provides help desk personnel with immediate information to pinpoint problems with network response time, loads, and equipment. Using NetSpy, a help desk attendant can quickly zero in on a user's terminal or application to determine whether a response time problem is caused by delays in the network or the host.

Management

NetSpy lets you set service level objectives and then provides you with response time distributions so that you may determine whether or not service level goals are being met.

NetSpy can produce reports that supply complete information on network performance and equipment usage for management. NetSpy also furnishes data on which terminals are accessing the system and which applications are being used, as well as planning information for improving service levels.

Network Capacity Planners

NetSpy provides data that planners can use to model or project network activity and growth, including network accounting statistics.

NetSpy offers a wide range of historical reports and online displays. For long-term trend analysis, in addition to normal logging functions, NetSpy creates SMF records that can be integrated into your performance reporting procedures.

With NetSpy's network modeling and recommendations component, planners can quickly evaluate the impact of new applications and increased transaction rates on the network.

Accounting Personnel

NetSpy provides two types of network accounting statistics. Session accounting collects network statistics from the start of a session to its end. Gateway accounting collects session statistics for SNI sessions.

Related Documentation

The Unicenter NetSpy Network Performance product is supported by the following documentation:

- *Unicenter Mainframe Installation Instructions*
- *Unicenter Mainframe Maintenance Instructions*
- *Unicenter NetSpy Network Performance Getting Started*
- *Unicenter NetSpy Network Performance Administrator Guide*
- *Unicenter NetSpy Network Performance User Guide*
- *Unicenter NetSpy Network Performance Messages Guide*
- *Unicenter NetMaster Network Performance for TCP/IP Implementation Guide*
- *Unicenter NetMaster Network Performance for TCP/IP Administrator Guide*
- *Unicenter NetMaster Network Performance for TCP/IP User Guide*

All manuals are available on the *Unicenter Mainframe Documentation Library CD-ROM*.

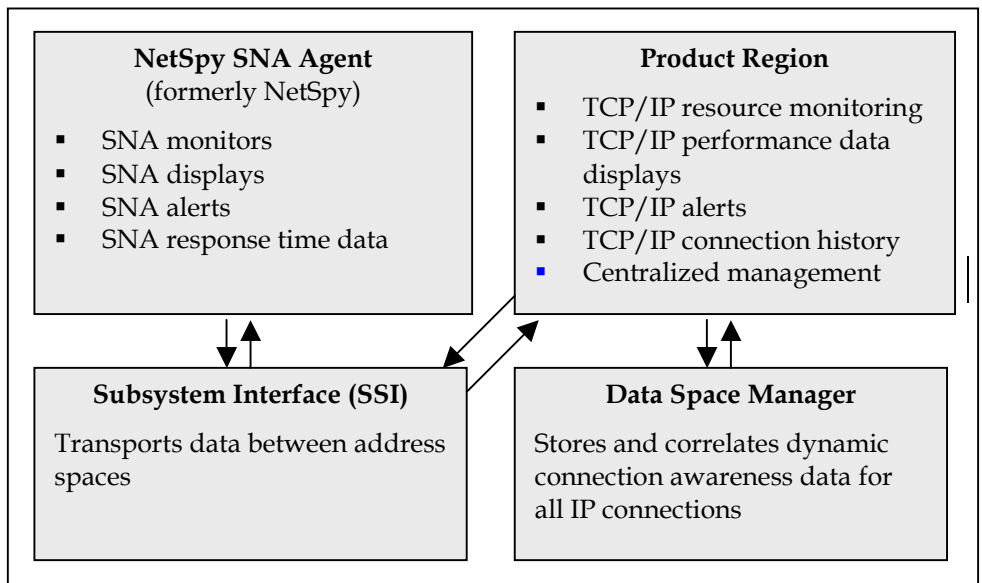
Release Summary

This chapter describes the new features and enhancements provided in Unicenter NetSpy Network Performance Version 6.0.

Note: Version 6.0 features are not supported in NetSpy for VM.

NetSpy 6.0 brings together the superior SNA monitoring capabilities of NetSpy and the advanced TCP/IP performance monitoring of NetMaster for TCP/IP. This combination of SNA and TCP/IP monitoring capabilities makes NetSpy the complete OS/390 and z/OS network performance management solution.

NetSpy Version 6.0 – Address Spaces (Regions)



New Primary Menu

From the new Unicenter NetSpy : Primary Menu you can access:

- SNA performance monitoring (NetSpy) functions
- TCP/IP performance monitoring functions
- Central functions for administering and customizing your NetSpy region

```
PROD----- Unicenter NetSpy : Primary Menu -----
Select Option ==>

M   - Monitors                                     Userid USER
H   - Historical Data                             LU      NMMAF088
D   - IP Network Diagnosis                       Time    13.56.50
U   - User Services                             TUE 11-SEP-2001
O   - Operator Console Services                 OPSYS   05390
A   - Administration and Definition             Window  1
SP  - SNA Performance (Appl ID NSD1VD1N)
X   - Terminate Window/Exit
```

Tip of the day: To browse SNA status codes enter /SNACODE at any ==> prompt.

(C) 1981,2001 Computer Associates International, Inc. All Rights Reserved.
F1=Help F2=Split F3=Exit F4=Return
 F9=Swap

TCP/IP Performance Enhancements

From the primary menu, you can access the Status Monitor : IP Resources panel (the IP resource monitor).

PROD----- Status Monitor : IP Resources -----					PROD-0000				
Command ==>					Scroll ==> PAGE				
D=Display H=History AL=Alerts L=Transient Log ?=List Cmds									
Resource	Class	System	Actual	Monitor	Alert	Max	Last	Next	
			Status	Status	Count	Sev	Samp	Samp	
FTPSRV32	ASMON	QAALLD1	ACTIVE	Ok	0	0	14:05	15:05	
OMPROUTE	ASMON	QAALLD1	ACTIVE	Ok	0	0	14:05	15:05	
OSNMPD	ASMON	QAALLD1	ACTIVE	Ok	0	0	14:05	15:05	
QANM1	ASMON	QAALLD1	INACTIVE	-	-	-	14:35	14:50	
SMTP32	ASMON	QAALLD1	ACTIVE	Ok	0	0	14:05	15:05	
SNMPQE	ASMON	QAALLD1	ACTIVE	Ok	0	0	14:05	15:05	
TCPIP38	ASMON	QAALLD1	ACTIVE	Ok	0	0	14:05	15:05	
ASSYGR11	CIP	QAALLD1	ACTIVE	Ok	0	0	14:05	15:05	
CIPSPPU	CIP	QAALLD1	ACTIVE	Ok	0	0	14:35	14:45	
CSM	CSM	QAALLD1	ACTIVE	Ok	1	1	14:40	14:45	
EE	EE	QAALLD1	ACTIVE	Ok	1	4	14:40	14:45	
OSAET0	OSA	QAALLD1	UNKNOWN	-	-	-	12:15	-	
OSATR0	OSA	QAALLD1	ACTIVE	Ok	0	0	12:05	-	
END									
F1=Help			F2=Split		F3=Exit		F4=Add		
F7=Backward			F8=Forward		F5=Find				
			F9=Swap						

Monitoring Critical IP Resources and Nodes

From the IP resource monitor, you can review detailed information about the performance of:

- Cisco channel cards
- Enterprise Extender
- 2216 routers
- Open System Adapters
- IBM and TCPaccess stacks
- Communication Storage Manager
- Address spaces with open ports

The type of information available to you includes:

- Device-specific displays
- Configuration information for devices
- IP connection history

Also, from the primary menu, you can access the IP Node Monitor. From this monitor you can review response time and availability data about your critical IP nodes.

```

PROD----- TCP/IP : IP Node Monitor -----
Command ==>>                                     Scroll ==> PAGE

                                     S=System Info H=History U=Update D=Delete
                                     .-- Last Ping --. Next
IP Address      Host Name           Status   Avg    Max    Time   Samp
192.168.19      assdd1.ca.com           OK       37     81    14:41  14:51
192.168.110.25  assymf10.ca.com        OK       37     81    14:41  14:51
192.168.110.26  FTI4500.ca.com         OK       17     20    14:41  14:51
192.168.110.27  CS for OS/390 V2R8     OK       15     24    14:41  14:51
192.168.110.28  CS for OS/390 V2R8     OK       14     27    14:41  14:51
192.168.110.29  FTI4500.ca.com         OK       22     27    14:41  14:51
192.168.110.30  CIPSPPU                OK       16     25    14:41  14:51
192.168.110.128 CIPSPPU                OK       26     38    14:41  14:51
192.168.110.129 assygr11.ca.com         OK       19     24    14:41  14:51
192.168.110.132 assyct07.ca.com         OK       18     23    14:41  14:51
192.168.110.134 assyct09.ca.com         OK       20     23    14:41  14:51
192.168.110.191 CIPSPPU                OK       20     22    14:41  14:51
192.168.110.193 assygr10.ca.com         OK       15     18    14:41  14:51
192.168.110.255 CIPSPPU                OK       14     18    14:41  14:51
**END**

F1=Help      F2=Split    F3=Exit     F4=Add      F5=Find
F7=Backward  F8=Forward  F9=Swap     F11=Right

```

For details about monitoring IP resources and nodes, see the *Unicenter NetMaster Network Management for TCP/IP User Guide*.

Other Enhancements for TCP/IP

Other TCP/IP enhancements include:

- Support for multiple TCP/IP stacks

NetSpy processes control statements during initialization for each stack to be monitored, establishes a connection, and collects requested data for those stacks. You can dynamically add, delete, or change the stacks being monitored. See the *Unicenter NetSpy Network Performance User Guide* for details.
- Correlated VTAM and TCP/IP statistics

Both TCP/IP and VTAM performance statistics from Telnet are correlated and displayed on the one panel, the List Telnet Connections panel.
- Historical reporting on FTP, Telnet, and client API connections
- Filterable connection lists for TN3270 and other TCP/IP connections
- Ability to issue TCP/IP, VTAM, and system commands from a console interface
- Ability to perform advanced TCP/IP monitoring through TCP/IP sockets using the NCL programming language

SNA Performance Enhancements

Significant enhancements to NetSpy's SNA monitoring capability are included in this release.

Integration with the NetMaster Alert Monitor

NetSpy alerts can now be viewed and actioned from the NetMaster alert monitor. The alert monitor provides an integrated, correlated event notification system that indicates to network operators that a condition has been detected and that some action needs to be taken. Alerts are presented in order of severity, depending on how often they occur.

From the alert monitor, you can initiate actions such as starting recovery procedures and creating trouble tickets, either automatically or manually.

Improved Availability

There is an online statistics display for NetSpy's most critical tuning parameters.

NetSpy has a new command and a new display that allows you to display the maximum values that were set at startup, and to display the current and maximum values, while NetSpy is active. This is another feature that will increase NetSpy's availability and enable it to be a monitor that can run 24 hours a day, 7 days a week.

It is now possible to restart various NetSpy subtasks to eliminate recycling the entire region when problems are encountered.

NetSpy has a new command to allow subtasks to be stopped and restarted. This command is also available from the console interface.

NeuPerformance Advisor Interface

NetSpy's new parameters let you customize and control the NeuPerformance Advisor interface. You can do such things as identifying the subsystem name and specifying which data will be passed to the NeuPerformance Advisor interface.

Other Enhancements for SNA

- Support for VTAM's expanded element addressing
NetSpy processes Expanded Element Addresses, if present.
- Automated operations can interface with NetSpy through a console interface
NetSpy will accept, parse, and act on commands entered through the MVS console interface. Responses are returned to the issuing console.
- Support for the four-digit years value in date parameters
NetSpy accepts and correctly processes the four-digit years.
- Support for NCP Version 7.7 and 7.8
NetSpy recognizes the data from NCP version 7.7 and 7.8 and includes it in the log records, data screens, and reports.
- Listings of start/init/alert/graph parameters during NetSpy's initialization
NetSpy will print out each control statement, as it is read, for the four different options. This listing will enable support to know what options NetSpy was started with, and it will enable clients to check that their parameters have been customized correctly.
- A signon message in the log when a user starts a session with NetSpy
NetSpy produces a message in the NetSpy log when a user starts a 3270 session.

- A date in the alert messages displayed on the console
Alert messages now have a date so you can easily identify when alerts happen.
- Control statements and parameters to eliminate optional zaps and undocumented options
Undocumented options were converted into standard parameters that clients can use without having to call support for details.
- N28CONV now converts record types D, E, F, M, P, and R
- Dropped support of GDDM (announced with NetSpy 5.3)

Administration and Customization Enhancements

The addition of the Management Services base provides the following functions for centralized administration and customization of your NetSpy region:

- An operator console
- Ability to control the authority and privileges of users
- Print management
- Communication between domains and programs
- Alert monitoring
- Broadcast messages
- Report writing
- Application development
- System support

For details of these facilities see the *Management Services User Guide*.

Installing and Implementing the NetSpy Product

This chapter provides an overview of how to install and implement the product. It refers to other manuals that provide detailed information about these tasks.

The product comprises the following four regions that work together to provide you with the complete solution to your network management needs:

- NetSpy SNA agent (previously known as CA-NetSpy) that performs SNA performance monitoring
- Subsystem Interface that provides in-memory communication between the product region, the NetSpy SNA agent, and the Data Space Manager
- Data Space Manager that stores connection awareness data for fast retrieval of TCP/IP connection information
- Product region where users log on and access SNA and TCP/IP product functions

Installation and Implementation Overview

The installation and implementation steps are detailed in the following sections:

[Step 1: Install and Set Up the Product](#)

[Step 2: Customize the NetSpy SNA Agent](#)

[Step 3: Implement the TCP/IP Interface](#)

[Step 4: Build the Environment to Manage Your TCP/IP Resources](#)

[Step 5: Implement Other Functions](#)

Step 1: Install and Set Up the Product

For detailed information, see the *Unicenter Mainframe Installation and Setup Instructions*.

- Unload the Install Utility from the product tape.
- Use the Utility to generate the jobs that you submit to install the product.
- Use the Utility to generate the jobs that you submit to set up the four regions of the product.
- After you set up the regions, you can start them and log on through the product region. During this initial session, **add a user ID for subsequent logon.**

Step 2: Customize the NetSpy SNA Agent

For detailed information, see the *Unicenter NetSpy Network Performance Administrator Guide* for the agent.

- Customize the initialization parameters in the INITPRM member.
- Customize the startup parameters in the STARTPRM member.
- Customize the alert parameters in the ALERTPRM member.
- Customize the graphic alert parameters in the GRAPHPRM member.
- Implement any optional features that you have enabled in the agent parameters.

Step 3: Implement the TCP/IP Interface

For detailed information, see the *Unicenter NetMaster Network Management for TCP/IP Implementation Guide (incorporating NetSpy and NetMaster Network Operations for TCP/IP)*.

Important! *It is not necessary to be licensed for or include Unicenter NetMaster Network Management for TCP/IP in your product region to collect TCP/IP performance information.*

- Configure the TCP/IP interface for the product.
- Enable FTP, TCP/IP connection, and Telnet event flow for connection awareness (see also [Step 5: Implement Other Functions](#) in this chapter).

Step 4: Build the Environment to Manage Your TCP/IP Resources

For detailed information, see the *Unicenter NetMaster Network Management for TCP/IP Implementation Guide (incorporating NetSpy and NetMaster Network Operations for TCP/IP)*.

Important! *It is not necessary to be licensed for or include Unicenter NetMaster Network Management for TCP/IP in your product region to collect TCP/IP performance information.*

- Log on to the product region, and customize the parameters for the region.
- Use the Express Setup Facility to discover and define the TCP/IP resources known to your system.
- Define a user ID as the administrator of the region and other user IDs as required. (For more information about security, see the *Unicenter NetMaster Network Management for TCP/IP Administrator Guide*.)

Step 5: Implement Other Functions

For detailed information, see the *Unicenter NetMaster Network Management for TCP/IP Administrator Guide (incorporating NetSpy and NetMaster Network Operations for TCP/IP)*.

- Set up connection awareness for TCP/IP connection events
- Customize the TCP/IP resources defined by the Express Setup Facility or define additional TCP/IP resources, which you can monitor by using the IP resource monitor.
- Define IP nodes, which you can monitor by using the IP node monitor.
- Link multiple regions to enable central monitoring of resources on different systems

Quick Tour

This quick tour takes you through some of the features of the Unicenter NetSpy Network Performance product.

About the Quick Tour

Important! *Ensure that you have completed all of the tasks listed in the chapter “Installing and Implementing the NetSpy Product” before taking this quick tour.*

In this quick tour you will:

- View a list of menu shortcuts
- List the IP resources defined to your region
- List the commands you can use
- List the stacks defined to your system
- Obtain a list of IP connections
- Review your stack monitor settings
- Monitor a stack
- Produce a graph of the number of IP packets delivered by a stack

Examining Your IP Details

The express setup detects the IP resources on your system. In this section you will review the list of IP resources defined by the express setup.

To list the IP resources on your system, do this:

1. Access your Unicenter NetSpy : Primary Menu.

```
PROD----- Unicenter NetSpy : Primary Menu -----  
Select Option ==>
```

```
M  - Monitors  
H  - Historical Data  
D  - IP Network Diagnosis  
U  - User Services  
O  - Operator Console Services  
A  - Administration and Definition  
SP - SNA Performance (Appl ID NETSPY)  
X  - Terminate Window/Exit
```

```
Userid USER01  
LU      UNIT01  
Time    08.48.45  
TUE 29-FEB-2002  
OPSYS   05390  
Window  1
```

Tip of the day: To browse SNA status codes enter /SNACODE at any ==> prompt.

```
(C) 1981,2001 Computer Associates International, Inc. All Rights Reserved.  
F1=Help      F2=Split      F3=Exit      F4=Return  
              F9=Swap
```

2. Enter a forward slash (/) at the ===> prompt. The CAS : Menu Shortcuts List panel is displayed. This panel lists and describes the panel shortcuts available. Shortcuts provide a fast way of navigating between panels.

```

PROD----- CAS : Menu Shortcuts List -----
Command ===>                                     Scroll ===> PAGE

                Select the required shortcut by placing an 'S' beside it

Shortcut  Description
/ACADMIN  SNA Access Services : Administration
/ADMIN    Administration : Primary Menu
/AFTMON   Active File Transfer Monitor
/ALADMIN  Alert Monitor : Administration Menu
/ALERTS   Alert Monitor
/ALHIST   Alert History
/ALLOC    List Allocated Files
/APING    APING a Control Point
/APPNDIR  Display APPN Directory Information
/APPNDLU  List Dependent LU Requestors
/APPNRTU  List RTP Pipes
/APPNTOP  Display APPN Subnetwork Topology Information
/APPNTRL  List Transport Resource List Entries
/ASADMIN  Automation Services : Administration Menu
/BCAST    Broadcast Services
/CAS      CAS : Maintenance Menu
/CASCMD   CAS : Command Definition Menu
F1=Help   F2=Split   F3=Exit    F4=Return   F5=Find     F6=Refresh
F7=Backward F8=Forward  F9=Swap

```

3. Press F8 (Forward) until the /IPMON shortcut is displayed.

```

PROD----- CAS : Menu Shortcuts List -----
Command ===>                                     Scroll ===> PAGE

                Select the required shortcut by placing an 'S' beside it

Shortcut  Description
/INMCDEF  List INMC Link Definitions
/INMCL    System Support : INMC Link Maintenance
/IPADMIN  TCP/IP : Administration Menu
/IPCON    TCP/IP : Connections
/IPDIAG   TCP/IP : Network Diagnosis
/IPHIST   TCP/IP : History Data
/IPMON    IP Resource Monitor
/IPMOND   Maintain IP Node Monitor Groups
/IPNODE   IP Node Monitor
/IPPKT    TCP/IP : Packet Tracing Menu
/IPTEST   Run TCP/IP Self Test
/LAN      IBM LAN Manager
/LEVELS   Product Component Software Levels
/LISTCON  List Connections for a Task
/LISTREG  List Linked Regions
/LISTTEL  List Telnet Connections
/LOADMIN  Activity Log Administration
F1=Help   F2=Split   F3=Exit    F4=Return   F5=Find     F6=Refresh
F7=Backward F8=Forward  F9=Swap

```

- Enter **S** in front of the /IPMON shortcut. The Status Monitor : IP Resources panel is displayed. This panel lists the IP resources defined to your region.

PROD----- Status Monitor : IP Resources -----							-PROD-0001	
Command ==>							Scroll ==> PAGE	
D=Display H=History AL=Alerts L=Transient Log ?=List Cnds								
Resource	Class	System	Actual	Monitor	Alert	Max	Last	Next
CD410DE1	ASMON	QANM18	ACTIVE	Ok	0	0	16:40	16:55
CSNM2	ASMON	QANM18	ACTIVE	Ok	0	0	16:40	16:55
CSNM3	ASMON	QANM18	INACTIVE	-	-	-	16:40	16:55
CSNM14	ASMON	QANM18	ACTIVE	Ok	0	0	16:40	16:55
CSNM27	ASMON	QANM18	ACTIVE	Ok	0	0	16:40	16:55
CSNM28	ASMON	QANM18	ACTIVE	Ok	0	0	16:40	16:55
DENM1	ASMON	QANM18	ACTIVE	Ok	0	0	16:40	16:55
DENM2	ASMON	QANM18	ACTIVE	Ok	0	0	16:40	16:55
DENM4	ASMON	QANM18	ACTIVE	Ok	0	0	16:40	16:55
DENM13	ASMON	QANM18	ACTIVE	Ok	0	0	16:40	16:55
FTPSRV32	ASMON	QANM18	ACTIVE	Ok	0	0	16:40	16:55
OMPROUTE	ASMON	QANM18	ACTIVE	Ok	0	0	16:40	16:55
OSNMPD	ASMON	QANM18	ACTIVE	Ok	0	0	16:40	16:55
CIPSPPU	CIP	QANM18	ACTIVE	Ok	0	0	16:40	16:55
CSM	CSM	QANM18	ACTIVE	Ok	0	0	16:40	16:55
EE	EE	QANM18	ACTIVE	Ok	0	0	16:40	16:55
OSA-B4	OSA	QANM18	ACTIVE	Ok	0	0	16:40	16:55
TCPICSD1	STACK	QANM18	ACTIVE	Ok	0	0	16:40	16:55
TCPIC52	STACK	QANM18	ACTIVE	Ok	0	0	16:40	16:55
TCPIP38	STACK	QANM18	ACTIVE	Ok	0	0	16:40	16:55
F1=Help	F2=Split	F3=Exit	F4=Add	F5=Find				
F7=Backward	F8=Forward	F9=Swap						

Tip: You can enter a shortcut from the ===> prompt on any panel.

5. Enter ? next to a STACK resource class. The Automation Services : Command List panel is displayed. This panel lists all of the commands available for this resource. The commands that are specific to a resource are displayed in blue at the top of the list.

```

PROD----- Automation Services : Command List -----
Command ==>                                         Scroll ==> HALF

                                Use 'S' to select the required Command

Command      Description
AL           View Alerts for a Resource
AM           Activate Monitoring
CL           Check Telnet LUs
CMD          Issue Modify to Stack
D            Display Resource Status
DG           Display Graphical Device Links
DL           Display Device Links
DP           Display Profile Configuration Libraries
ERL          Browse TCP/IP Error Log
H            Show Performance History
IC           IP Connections
ICA          IP Connections for all Applications
IM           Inactivate Monitoring
IP           View Stack IP Performance History
IPM          View Stack IP Performance Metrics
LA           List Applications with IP Connections
O            Execute Obeyfile
F1=Help      F2=Split    F3=Exit      F4=Return    F5=Find      F6=Refresh
F7=Backward  F8=Forward   F9=Swap

```

6. Select the IPM command. The TCP/IP : Stack IP Performance Metrics panel is displayed. This panel displays a current analysis of the stack.

```

PROD----- TCP/IP : Stack IP Performance Metrics -Columns 00001 00079
Command ===>                               Scroll ===> PAGE

Stack Address ..... 123.123.123.01

***** TOP OF DATA *****
Stack Name ..... CS for OS/390 V2R8
Stack Procedure Name ..... TCPIP38
Date Started ..... SUN 31-SEP-2001 18:37:58.8
Address Space ID ..... 82 (decimal)

TCP Statistics

  Buffer Size - Receive ..... 16384
               Send ..... 16384
  Connections - Maximum Supported ..... DYNAMIC
               Currently Established ... 70
               Resets ..... 521
               Active Opens ..... 1352
               Passive Opens ..... 4316
               Failures ..... 12268
  Segments - Sent ..... 909719

F1=Help      F2=Split      F3=Exit      F5=Find      F6=Refresh
F7=Backward  F8=Forward   F9=Swap

```

7. Enter == at the ===> prompt to return to the Unicenter NetSpy : Primary Menu.

Listing Telnet Connections

To view a list of Telnet Connections, do this:

1. From the primary menu, enter the panel path, **D.C.LC** at the **==>** prompt. The TCP/IP : Connection List Criteria panel is displayed. This panel provides input fields that allow you to define which IP connections to list.

```
PROD----- TCP/IP : Connection List Criteria -----
Command ==>                                         Function=Search
```

```
Connection Criteria
Remote host .....
Remote port .....
Local port .....
Application name ...
Task name .....
LU name .....
User ID .....
TCP/IP stack .....+
Include history? ... NO
Fast search? ..... YES
```

F1=Help

F2=Split

F3=Exit
F9=Swap

F6=Action

Tip: .Panel paths provide an alternative to shortcuts for navigating panels. A panel path is constructed by linking the required menu options with periods.

2. Press F6 (Action). The TCP/IP : Connection List panel is displayed. This panel displays information about the current state of the active connections.
3. Press F11 (scroll right) to display more connection details on this panel.

```

PROD----- TCP/IP : Connection List -----Stack: *MULTIPLE*
Command ==> Scroll ==> PAGE
GP0006 Function key F10 is not active in this window
Line 1 of 16 Refresh Every ... Seconds
S=View L=Log
Foreign Host Port Local Host LPort LU name User ID TaskName
172.16.122.208 3231 234.210.110.25 23 SSTCP041 TCPIP38
172.16.122.140 2440 234.210.110.25 21 USER01 FTPSRV32
192.168.110.136 2605 234.210.110.25 2860 TEST
172.16.122.208 3164 234.210.110.25 23 SSTCP007 TCPIP38
172.16.122.50 1110 234.210.110.25 23 SSTCP040 TCPIP38
172.16.123.22 8044 234.210.110.25 2746 XC300DE1
172.16.123.22 8044 234.210.110.25 2644 XC300DE1
172.16.122.50 1105 234.210.110.25 23 SSTCP049 TCPIP38
172.16.122.138 1186 234.210.110.25 23 SSTCP042 TCPIP38
172.16.122.50 1102 234.210.110.25 23 SSTCP029 TCPIP38
172.16.122.163 1273 234.210.110.25 23 SSTCP053 TCPIP38
172.16.122.61 2636 234.210.110.25 1458 TEST
172.16.122.64 1144 234.210.110.25 23 SSTCP032 USER02 TCPIP38
172.16.122.166 1630 234.210.110.27 23 SSTCP052 TCPIP38
F1=Help F2=Split F3=Exit F6=Refresh
F7=Backward F8=Forward F9=Swap F11=Right

```

4. Press F1 (Help). The online help for this panel is displayed. Use the help for information on the fields and actions available on this panel.
5. Enter == at the ==> prompt to return to the Unicenter NetSpy : Primary Menu

Examining Stack Monitoring Setup

The IP resources defined to your system by the express setup are monitored at regular intervals.

To examine how the stack monitor was set up by the express setup, do this:

1. Enter **/RADMIN** at the **==>** prompt. The Automation Services : Resource Administration panel is displayed. You can use the options on this panel to set up and maintain your system image.

```

PROD----- Automation Services : Resource Administration -----/RADMIN
Select Option ==>

R   - Resources
P   - Processes
GP  - Global Processes
I   - System Images
T   - Template Definition Menu
AD  - Assisted Resource Definition Menu
X   - Exit

System Name ..+ PROD      ( Required R P  )
Version .....+ 0001      ( Required R P  )


F1=Help      F2=Split      F3=Exit      F4=Return
F9=Swap

```

2. Enter **R** at the **==>** prompt. The ResourceView : Resource Definition panel is displayed. This panel lists the resources that you can define and maintain in the specified image.

3. Enter **S** next to the resource class STACK. The ResourceView : TCP/IP Stack List panel is displayed. This panel lists the stacks defined to your system.
4. Enter **S** to select one of the stacks. The ResourceView : Panel Display List panel is displayed. This panel lists the six panels that define your stack details.

```
PROD----- ResourceView : Panel Display List -----
Command ==>                                         Scroll ==> PAGE

                                         Use 'S' to select panel(s) to be displayed

Panel Description
TCP/IP Stack General Description
STACK TEST Monitoring Definition
STACK TEST Stack Management Definition
STACK TEST Status Monitor Message Details
STACK TEST Automation Log Details
STACK TEST Owner Details
**END**

F1=Help      F2=Split    F3=Exit      F4=SAVESEQ   F5=Find      F6=Refresh
F7=Backward  F8=Forward   F9=Swap
```

5. Select the STACK *name* Monitoring Definition panel. The ResourceView : STACK *name* Monitoring Definition panel is displayed. This panel defines what performance attributes of the stack are monitored and how often.

```
PROD----- ResourceView : STACK TEST Monitoring Definition -----TEST-0001
Command ==>

Monitor Rate ..... 15           Minutes (5-60)
Reporting Level ..... TREND      (None, Trend, Summary or Detail)
TCP Port(s) .....
UDP Port(s) .....

Attribute          Alert Summary          Status
CPU%               ACTIVE
EXCP               ACTIVE
JobCount           ACTIVE
SRBCPU             ACTIVE
TaskCPU            ACTIVE
TotalCPU           ACTIVE
Connections        INACTIVE
PortStatus         INACTIVE

F1=Help    F2=Split    F3=Exit    F4=Edit
F7=Backward F8=Forward  F9=Swap    F10=ViewLst F11=Panels
```

6. Examine how the stack is being monitored.

Tip: Press F1 (Help) for a description of the monitored attributes.

7. Enter == at the ==> prompt to return to the Unicenter NetSpy : Primary Menu.

Viewing the Monitoring Results

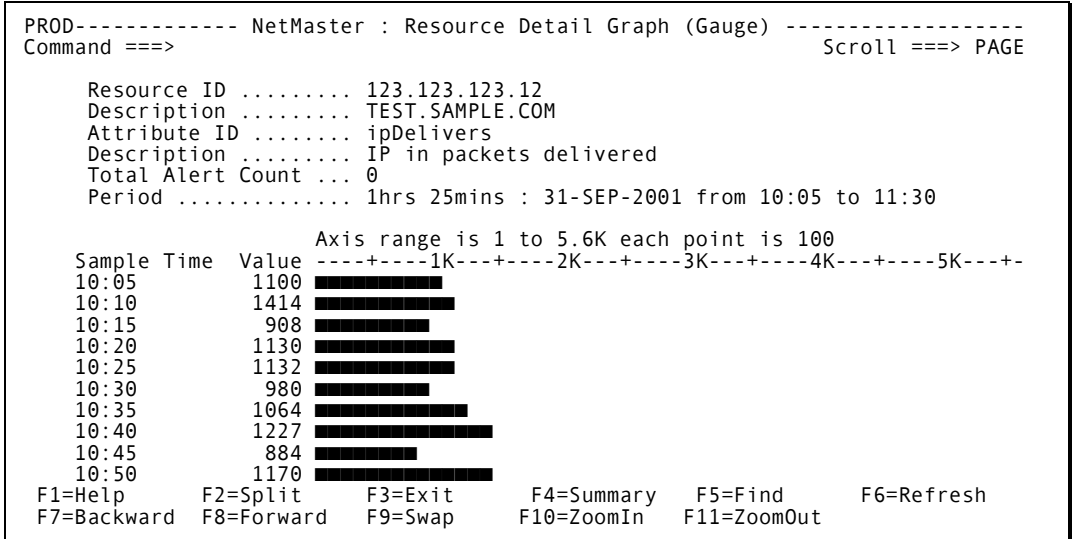
***Important!** The monitoring examined in Examining Stack Monitoring Setup must have been running for more than an hour before doing this task to allow time for summary data to be gathered.*

To view the results of stack monitoring, do this:

- 1. Enter **/IPMON** at the **===>** prompt. The Status Monitor : IP Resources panel is displayed. This panel lists the IP resources monitored by your region.
- 2. Enter **IP** in front of the Stack resource. The TCP/IP : Monitor Stack IP Performance History panel is displayed. This panel shows the results of the stack monitoring.

PROD----- TCP/IP : Monitor Stack IP Performance History -----										-----	
Command ==>						Scroll ==> PAGE					
Resource ID 172.162.0.1											
Description sample.test.com											
Current Alerts 0											
						E=Expand C=Contract S/=Summary D=Detail					
						Alerts Last					
Attribute/Qualifier		Open	Total	Samples	Sample	Value	Type				
d	ipAddrErrors		0	14	10:10	102	GAUGE				
	ipDelivers		0	14	10:10	348	GAUGE				
	ipDgrmsForwarded		0	14	10:10	0	GAUGE				
	ipDgrmsUnknwnPro		0	14	10:10	0	GAUGE				
	ipDiscards		0	14	10:10	0	GAUGE				
	ipFragCreates		0	14	10:10	0	GAUGE				
	ipFragFailed		0	14	10:10	0	GAUGE				
	ipFragOk		0	14	10:10	0	GAUGE				
	ipHeaderErrors		0	14	10:10	0	GAUGE				
	ipOutDiscards		0	14	10:10	0	GAUGE				
	ipOutNoRoutes		0	14	10:10	0	GAUGE				
	ipOutRequests		0	14	10:10	320	GAUGE				
	ipReasmFailed		0	14	10:10	0	GAUGE				
F1=Help		F2=Split		F3=Exit		F4=Expand		F5=Find		F6=AutoRfsh	
F7=Backward		F8=Forward		F9=Swap				F11=Right		F12=ByQual	

- Enter **D** next to the ipDelivers Attribute. The NetMaster : Resource Detail Graph (Gauge) panel is displayed. This panel shows the number of IP packets delivered by this stack for each sampled interval since monitoring started.



- Enter **==** at the **==>** prompt to return to the Unicenter NetSpy : Primary Menu.

For more information about the TCP/IP functions of NetSpy, see the *Unicenter NetMaster Network Management for TCP/IP User Guide*.

Index

A

accessing
 NetSpy, 2-2
 SNA monitoring, 2-2
 TCP/IP monitoring, 2-2

B

benefits of NetSpy
 to help desk personnel, 1-6
 to management, 1-7
 to network capacity planners, 1-7
 to network control center staff, 1-5
 to systems programmers, 1-6

C

commands
 issuing, 2-5
 system, 2-5
 TCP/IP, 2-5
 VTAM, 2-5

F

FTP, 2-5, 3-3

I

installation
 number of regions, 3-1
 overview of procedure, 3-2

L

load balancing, 1-3

M

multiple regions, 3-4

N

NCP, 1-5, 1-6

NetSpy

- address spaces, 2-1
- availability, 2-6
- benefits, 1-1, 1-5
- for VM, 2-1
- functions, 1-1
- navigating, 4-1
- new features, 2-1
- TCP/IP functions, 4-1

network

- capacity, 1-3
- efficiency, 1-2
- expansion, 1-4
- modeling, 1-4, 1-6, 1-7

NeuPerformance, 2-7

S

service level agreements, 1-3

SMF, 1-5

- files, 1-7

SNA

- alert monitor, 2-6
- ALERTPRM member/file, 3-3
- alerts, 3-3
- customizing initialization parameters, 3-3
- customizing startup parameters, 3-3
- graphic alerts, 3-3
- GRAPHPRM member/file, 3-3
- INITPRM member/file, 3-3
- monitoring, 2-6
- STARTPRM member/file, 3-3

statistics

- accounting, 1-7
- NCP, 1-5
- TCP/IP, 1-5, 2-5
- VTAM, 1-5, 2-5

T

TCP/IP

- monitoring, 2-3, 2-5
- nodes, 2-4
- resources, 2-3
- sockets, 2-5
- stacks, 2-5

Telnet, 2-5, 3-3

V

VTAM

- expanded element addressing, 2-7
- statistics, 2-5